Sample audit programme

Data protection

Technical and organisational measures

12 audit steps · GDPR

12 audit steps with criterion, reference, procedure and expected evidence. 8 documents to request and the typical findings.

GDPR Art. 32(1) and (2) · GDPR Art. 32(1) · GDPR Art. 32(1)(a) · GDPR Art. 32(1)(b) · ISO/IEC 27001:2022 Annex A 5.15 · ISO/IEC 27001:2022 Annex A 8.15 · BSI OPS.1.1.4 · GDPR Art. 32(1)(c) · GDPR Art. 32(1)(d) · GDPR Art. 32(4) · GDPR Art. 28(1) and (3) · GDPR Art. 28(3)(h) · GDPR Art. 33(1) and (5)

Audit objective and scope

The audit assesses whether controllers and processors ensure a level of protection for personal data appropriate to the risk: risk consideration, encryption and pseudonymisation, confidentiality, integrity, availability and resilience of systems, restoration after incidents and regular review. It also assesses whether employees handle data only on instruction and whether processors are involved appropriately.

SCOPE

- Processing activities involving personal data, selected by risk, and the systems used for them
- Technical measures such as encryption, access protection, backup and logging
- Organisational measures such as policies, training, commitments and incident processes
- Out of scope: lawfulness of processing, data subject rights and transfers to third countries, unless agreed separately

Audit steps 1 to 3

Step 01

GDPR Art. 32(1) and (2)

The risk to the rights and freedoms of data subjects is assessed for the processing activities; the assessment takes account of likelihood and severity and is current.

Procedure Review the risk assessment for five processing activities and check its currency and how the level of protection is derived.

Evidence Record of processing activities, risk assessments

Step 02

GDPR Art. 32(1)

The measures are documented and proportionate to the risk, taking account of the state of the art and the costs of implementation.

Procedure Read the catalogue of measures and trace the allocation of measures to risk for three processing activities.

Evidence Measures concept, allocation of risk and measure

Step 03

GDPR Art. 32(1)(a)

Personal data is encrypted or pseudonymised where appropriate, in storage and in transit.

Procedure Check encryption settings for databases, backups, mobile devices and transmission paths in a sample.

Evidence Configuration extracts, encryption and pseudonymisation concept

Audit steps 4 to 6

Step 04 — GDPR Art. 32(1)(b); ISO/IEC 27001:2022 Annex A 5.15

Confidentiality is secured by an authorisation concept: access only for authorised people, on a need basis, with regular review.

Procedure Compare authorisations on systems holding personal data with the concept and review the last review.

Evidence Authorisation concept, rights extracts, review record

Step 05 — GDPR Art. 32(1)(b); ISO/IEC 27001:2022 Annex A 8.15

Integrity of data and systems is secured, for example through change protection, logging and checks for unauthorised alteration.

Procedure Check logging of changes to data sets and protection of the logs in two systems.

Evidence Logging configuration, evaluations

Step 06 — GDPR Art. 32(1)(b); BSI OPS.1.1.4

Availability and resilience of systems are secured through redundancy, capacity planning and protection against malware.

Procedure Compare availability requirements with the technical implementation and check coverage of malware protection.

Evidence Architecture overview, availability reports, coverage of protection software

Audit steps 7 to 9

Step 07 GDPR Art. 32(1)(c)

After a physical or technical incident, availability of and access to data can be restored quickly; restoration is tested.

Procedure Read the backup and restoration concept and review the results of the last restoration test.

Evidence Backup concept, record of the restoration test

Step 08 GDPR Art. 32(1)(d)

The effectiveness of the measures is tested, assessed and evaluated regularly under a defined procedure; results lead to measures.

Procedure Review the audit plan and reports of the last twelve months and follow up the implementation of measures.

Evidence Audit plan, reports of internal and external audits, action list

Step 09 GDPR Art. 32(4)

People with access to personal data process it only on instruction and are bound to confidentiality and trained.

Procedure Check commitment statements and training records for a sample of employees.

Evidence Commitment statements, training records, instructions

Audit steps 10 to 12

Step 10 GDPR Art. 28(1) and (3)

Contracts with processors regulate technical and organisational measures, binding instructions, sub-processing and audit rights.

Procedure Review the contracts of three processors against a checklist and compare the annexes on measures with practice.

Evidence Processing contracts, annexes on measures, checklist

Step 11 GDPR Art. 28(3)(h)

Compliance by processors is monitored, for example on the basis of evidence or audits.

Procedure Review evidence and checks of the last twelve months for essential processors.

Evidence Certificates, audit reports, records of checks

Step 12 GDPR Art. 33(1) and (5)

Personal data breaches are detected, documented and assessed and reported within the deadline.

Procedure Check the procedure for data breaches and review documentation and reports of the last twelve months.

Evidence Procedure, documentation of breaches, reports

Document request list

Request these 8 documents before you start

1. Record of processing activities
2. Risk assessments for the processing activities in the sample
3. Measures concept with allocation to risk
4. Authorisation concept and rights extracts
5. Encryption and pseudonymisation concept
6. Backup concept and record of the last restoration test
7. Processing contracts with annexes
8. Audit plans and reports on the review of measures

TYPICAL FINDINGS

- Measures are not tied to the risk of the processing activity; one standard package applies to all.
- The authorisation concept is not implemented, and too many people access data sets with personal data.
- Backups are not encrypted, and restoration tests are missing.
- The effectiveness of the measures is not reviewed regularly.
- Annexes on technical and organisational measures at processors are outdated or general.
- Employees are not demonstrably committed and trained.

Sample audit programme library

29 sample audit programmes online

proauditmap.com/en/audit-programs/

Full audit package in ProAuditMap

proauditmap.com

ProAuditMap

Sample provided without warranty and not legal advice. Laws, regulations and standards appear only as references, no normative text is reproduced. Adapt scope and depth to your organisation, your risks and the current version of the provisions that apply to you before use.
Last updated: 13 October 2026